MOTHERSHIP PRODUCTIONS LIMITED
DATA PROTECTION POLICY

You must read this Policy because it gives important information about:
• the data protection principles with which Mothership must comply when collecting, handling, processing, transferring or storing Personal Data, including customer, employee, supplier and partner data; • what is meant by Personal Data and Special Categories of Personal Data; • how we gather, use and (ultimately) delete Personal Data and Special Categories of Personal Data in accordance with the data protection principles; • what your obligations are where you Process Personal Data on our behalf; and • the consequences of failure to comply with this Policy.

Introduction

This Policy sets out how Mothership Productions Limited ("**we**", "**our**", "**us**", "**Mothership**") handles the Personal Data of employees, agency and contingent workers, suppliers, partners, clients, contributors, website visitors and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, supplier and partner contacts, clients, contributors, website visitors or any other Data Subject.

This Policy applies to all Mothership Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for Mothership to comply with applicable law. Your compliance with this Policy is mandatory. Related Policies and Procedures are available to help you interpret and act in accordance with this Policy. You must also comply with all such Related Policies and Procedures. Any breach of this Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Policy, or otherwise, then you must comply with the Related Policies and Procedures.

This Policy (together with Related Policies and Procedures) is an internal document and must not be shared with third parties, customers, suppliers, partners, or regulators without prior authorisation from the Head of Production.

Capitalised terms used in this document shall have the meanings given to them in Annex A.

Scope

The lawful treatment of Personal Data ensures confidence in the organisation and provides for successful business operations. Protecting the confidentiality and security of Personal Data is a critical responsibility that we always take seriously. Mothership is exposed to potential fines of up to £17.5million or 4% of total worldwide annual turnover (whichever is higher and depending on the breach), for failure to comply with the provisions of Data Protection Legislation.

All Directors are responsible for ensuring all Mothership Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The Head of Production is responsible for overseeing this Policy and, as applicable, developing Related Policies and Procedures.

Please contact the Head of Production with any questions about the operation of this Policy or Data Protection Legislation, or if you have any concerns that this Policy is not being or has not been followed. You must always contact the Head of Production in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process Personal Data,

b) if you need to rely on Consent and/or need to capture Explicit Consent,

c) if you need to draft a Privacy Notice,

d) if you are unsure about the retention period for the Personal Data being Processed,

e) if you are unsure about what security or other measures you need to put in place to protect Personal Data,

f) if there has been a Personal Data Breach,

g) if you are unsure on what basis to transfer Personal Data outside the UK,

h) if you need any help dealing with a request from a Data Subject,

i) whenever you are engaging in a significant new, or change to an existing, Processing activity which is likely to require a DPIA, or you plan to use Personal Data for a purpose other than the purpose it was collected for,

j) if you are planning any activities which involve Automated Processing including profiling or Automated Decision-Making,

k) if you need help complying with applicable law when carrying out direct marketing activities, or

l) if you need help with due diligence or contracts needed to share Personal Data with third parties (including our suppliers/vendors).

Personal Data Protection Principles

We follow the principles relating to Processing of Personal Data set out in Data Protection Legislation which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);
- collected only for specified, explicit and legitimate purposes (**Purpose Limitation**);
- adequate, relevant and limited to what is necessary for the purposes for which it is Processed (**Data Minimisation**);
- accurate and where necessary kept up to date (**Accuracy**);
- not kept in a form which allows the identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**);
- Processed in a way that ensures its security using appropriate technical and organisational measures (**Security, Integrity and Confidentiality**);
- not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**); and
- made available to Data Subjects and allows Data Subjects to exercise their rights in relation to their Personal Data (**Data Subject's Rights and Requests**).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

Lawfulness, Fairness and Transparency

Lawfulness and Fairness

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

Data Protection Legislation allows Processing for specific lawful purposes, some of which are set out below:

- the Data Subject has given his or her Consent,
- the Processing is necessary for the performance of a contract with the Data Subject, to meet our legal compliance obligations,
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we

process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

You must identify and document the legal ground being relied on for each Processing activity.

Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in Data Protection Legislation (some of which are set out above), which include Consent.

A Data Subject Consents to Processing of their Personal Data if they clearly indicate agreement either by a statement or positive action to the Processing. Consent requires positive action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and their withdrawal must be honoured promptly. You may need to obtain Consent again if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When Processing Special Categories of Personal Data or Criminal Convictions Data, we will rely on a legal basis for Processing other than Explicit Consent or Consent, if possible. However, where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You must keep records of all Consents in accordance with Related Policies and Procedures so that Mothership can demonstrate compliance with Consent requirements.

Transparency (Notifying Data Subjects)

Data Protection Legislation requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information is usually provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects (including for human resources or employment purposes) we must provide the Data Subject with all the information required by Data Protection Legislation including the identity of the Controller and how and why we will use that Personal Data. through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (e.g., from a third party or publicly available source), we must provide the Data Subject with all the information required by Data Protection Legislation as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected, and is being shared, by the third party in accordance with Data Protection Legislation

We have prepared various Privacy Notices which may be used depending on the circumstances. Please contact the Head of Production if you have any questions regarding Privacy Notices.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes (and they have consented where Consent is the lawful basis relied upon).

Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when required to do so to perform your job. You must not Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect data which you do not absolutely need. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for the specified purposes, it is deleted or anonymised in accordance with Mothership's **Data Retention Policy**.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to correct or destroy inaccurate or out-of-date Personal Data.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which allows the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it (including for the purpose of satisfying any legal, accounting or reporting requirements).

Mothership will maintain retention policies and procedures to ensure Personal Data is deleted once it is no longer required for the purposes for was it was Processed unless Mothership is legally required to keep such data for a minimum time. You must comply with Mothership's **Data Retention Policy**.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all Mothership's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Security Integrity and Confidentiality

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly review and test the effectiveness of those safeguards to ensure the security of our Personal Data. You are responsible for protecting the Personal Data we hold. You must apply appropriate security measures to protect Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data.

You must follow all procedures and technologies we put in place to ensure the security of all Personal Data from the point of collection to the point of destruction. You may only share Personal Data with third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it,

b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed, and

c) Availability means that authorised users can access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the safeguards we implement and maintain to protect Personal Data.

Reporting a Personal Data Breach

Data Protection Legislation requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain circumstances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Head of Production using the **Breach Reporting Form** and follow the **Data Breach Protocol**. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer Limitation

Data Protection Legislation restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by Data Protection Legislation is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different

country.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

a) the UK government has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

b) appropriate safeguards are in place (such as binding corporate rules (BCR), standard contractual clauses approved by the UK government, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Head of Production;

c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in Data Protection Legislation including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Please contact the Head of Production if you have any questions about transfers of Personal Data outside the UK.

Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time,

b) receive certain information about the Mothership's Processing activities,

c) request access to their Personal Data that we hold,

d) prevent our use of their Personal Data for direct marketing purposes,

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to correct inaccurate data or to complete incomplete data,

f) restrict Processing in specific circumstances,

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest,

h) request a copy of an agreement under which Personal Data is transferred outside of the UK,

i) object to decisions based solely on Automated Processing, including profiling (ADM),

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else,

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms,

l) make a complaint to the supervisory authority, and

m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the Head of Production in accordance with the **Data Subject Requests Procedure.**

Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Mothership must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy,

b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects,

c) integrating data protection into internal documents including this Policy, Related Policies and Procedures, or Privacy Notices,

d) regularly training Mothership Personnel on Data Protection Legislation, this Policy, Related Policies and Procedures and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIAs and Personal Data Breaches. Mothership must maintain a record of training attendance by Mothership Personnel, and

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

Record Keeping

Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate records reflecting our Processing. These records should include, at a minimum, the name and contact details of the Controller and the DPO (if relevant), clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

Training and Audit

We are required to ensure all Mothership Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must complete all mandatory data privacy related training.

You must regularly review all the systems, processes, and personnel under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate measures (such as Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

- the current state of the art,
- the cost to implement such measures,
- the nature, scope, context and purposes of the Processing of Personal Data, and
- the risks to the rights and freedoms of Data Subjects posed by the Processing.

Mothership must also conduct DPIAs in respect to any high-risk Processing.

You should conduct a DPIA (and discuss your findings with the Head of Production) when implementing major system or business change programs involving the Processing of Personal Data including:

- changes to existing, or use of new, technologies, programs, systems or processes,
- Automated Processing including profiling and ADM,
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data, or
- large-scale, systematic monitoring of a publicly accessible area (for example, use of CCTV).

A DPIA must include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate,
- an assessment of the necessity and proportionality of the Processing in relation to its purpose,

- an assessment of the risk to individuals, and
- the risk mitigation measures in place and demonstration of compliance.

You must comply with the **Data Protection Impact Assessment Guidelines**.

Automated Processing (Including Profiling) and Automated Decision-Making

Generally, ADM is prohibited when it produces a legal or similar significant effect on an individual unless:

a) a Data Subject has Explicitly Consented,

b) the Processing is authorised by law, or

c) the Processing is necessary for the performance of, or entering into, a contract.

If a decision is based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and likely consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling), or ADM activities are undertaken.

Direct Marketing

We are subject to certain laws and rules when marketing to customers, or other third parties.

For example, a Data Subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception in the UK for existing customers known as the "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services,

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject,

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place,

d) the transfer complies with any applicable cross border transfer restrictions, and

e) a fully executed written contract that contains clauses mandated by Data Protection Legislation has been signed.

Review of this Policy

We keep this Policy under regular review in accordance with the Ownership, Implementation and Revision History set out at Annex C. This Policy does not override any applicable national data privacy laws and regulations in countries where Mothership operates. For further information about our compliance with Data Protection Legislation, please see the Related Policies and Procedures listed in Annex B or contact our Head of Production at gudren@mothershiptv.co.uk

Annex A- Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. Data Protection Legislation prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Legislation. We are the Controller of all Personal Data relating to our Mothership Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Legislation: means the UK GDPR, the UK Data Protection Act 2018 (**DPA 2018**), and the Privacy and Electronic Communications Regulations 2003 (**PECR**).

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under Data Protection Legislation.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Mothership Personnel: all directors, officers, employees, agency and contingent workers, members and others of Mothership.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal

data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's attributes, actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Legislation.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when Mothership collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies and Procedures: Mothership's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, as set out at Annex B

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.